Cybersecurity in Civil Aviation – Threat Landscape and Vulnerability Assessment of Attack Vectors

Alexander Lawall
IU International University of Applied Science
Erfurt, Thüringen, Germany
alexander.lawall@iu.org

***Abstract*—The digital transformation of civil aviation has introduced significant cybersecurity risks across interconnected systems such as avionics, air traffic control, and airport infrastructure. This paper examines the evolving threat landscape by identifying key threat actors, attack vectors, and system vulnerabilities. Using a qualitative approach based on expert interviews, the study reveals critical weaknesses in satellite communications, Automatic Dependent Surveillance–Broadcast (ADS-B), and legacy ground infrastructure. Results indicate high susceptibility to cyberattacks due to insufficient encryption, system fragmentation, and outdated protocols. The findings highlight the need for targeted risk assessments, standardized cybersecurity frameworks, and international collaboration to enhance aviation resilience.**

Keywords-Civil Aviation; Cybersecurity; Threat Landscape; Vulnerability Assessment; Attack Vectors; Critical Infrastructure.

I. Introduction

Digital transformation in civil aviation broadens the cyber threat landscape by exposing critical systems to significant vulnerabilities. Ten studies document that key aviation components—including communication, navigation, surveillance, and IT networks—lack robust security measures. For example, researchers report that wireless communication systems are inherently insecure [1] and that aeronautical communication standards rarely incorporate cybersecurity requirements [2]. Authors examining aircraft IT systems note substantial gaps in secure software design and communication practices [3], while studies targeting air traffic management (ATM) propose extended threat models to capture interdependent risks [4]. An analysis of ten identified attack vectors indicates that seven bear high potential impact (e.g., Global Navigation Satellite Systems (GNSS) spoofing, malware injection, ransomware, and ADS-B exploitation) and that detection capabilities mostly remain limited or moderate. Complementary approaches — such as novel risk assessment frameworks [5] and threat taxonomies [6] — illustrate efforts to systematically assess evolving challenges, including those emerging with urban air mobility and unmanned aerial systems [7].

This paper addresses three core research questions:

RQ1 *"Who are the relevant threat actors targeting civil aviation?"*

RQ2 *"What are the critical attack vectors exploited in this domain?"*

RQ3 *"How vulnerable are current aviation systems to these evolving threats?"*

This systematic review examines cybersecurity challenges across commercial aviation systems, encompassing both airborne and ground-based infrastructures [3], [8]. The analysis covers critical aviation components including Communication, Navigation, and Surveillance (CNS) systems, air-ground communication, radio navigation aids, and aeronautical surveillance systems [5]. The research methodology combines systematic reviews with both theoretical and empirical approaches [1], incorporating qualitative analysis through expert perspectives [9] and comprehensive threat assessments [4]. This multi-faceted approach enables a thorough examination of cybersecurity vulnerabilities in modern aviation systems, from aircraft information technology to ATM infrastructure [3], [10].

The paper is structured as follows: Section I introduces the cybersecurity challenges in civil aviation and formulates the key research questions. Section II presents the qualitative research methodology based on expert interviews. In Section III, we analyze the threat landscape by identifying prominent threat actors and their motivations. Section IV categorizes and evaluates the most relevant attack vectors and system vulnerabilities. Section V synthesizes expert insights and identifies key technical and organizational security gaps. Finally, Section VI concludes with the main findings, answers the research questions, and offers recommendations and future research directions.

II. Methodology

This research employs a qualitative methodology to investigate the cybersecurity threat landscape and vulnerabilities in civil aviation systems. The approach was chosen due to the complexity and sensitivity of the topic, which benefits from expert-based insights rather than purely quantitative data.

A. Research Design

The study follows an exploratory and descriptive design. The primary objective was to gather structured knowledge about realistic cyber threats, system vulnerabilities, and the expert perception of risk within the aviation domain. Given the limited publicly available data and operational sensitivity of aviation systems, expert interviews were deemed the most suitable method for data collection.

 ISBN: 978-1-68558-286-9

B. Expert Selection and Sampling

A purposive sampling strategy was employed to identify individuals with relevant professional expertise. Selection criteria included:

- Professional background in civil aviation, ATM, or aircraft systems.
- Specific experience in cybersecurity, cyber risk assessment, or information security.
- Academic or consulting roles with publications or projects in the aviation cybersecurity field.

The experts represented organizations such as aviation authorities, cybersecurity consultancies, aviation software vendors, and research institutions. All participants had more than five years of relevant work experience.

C. Interview Design and Procedure

Semi-structured interviews were conducted to ensure comparability while allowing for flexible and in-depth discussion. The interview guide included thematic blocks related to:

- Identification of relevant threat actors.
- Perception of technical vulnerabilities in airborne and ground systems.
- Assessment of communication protocol security (e.g., ACARS, ADS-B).
- Evaluation of organizational cybersecurity challenges.

Interviews were conducted via video conferencing and lasted between 30 and 60 minutes. With consent, all sessions were recorded and transcribed.

The expert sample comprised five aviation professionals serving as pilots/copilots on aircraft such as the Airbus A320, A330/340, and the CRJ-900. These individuals possessed an average flight experience ranging from 6,000 to 9,000 hours, indicating a high level of operational expertise. All participants were employed by German commercial airlines, providing a consistent organizational backdrop. The interviews focused on critical aspects of aviation cybersecurity, specifically addressing airborne systems, ground infrastructure, and communication links. GNSS, avionics systems, the Aircraft Communications Addressing and Reporting System (ACARS), and threats related to Instrument Landing System (ILS) spoofing are examples.

D. Data Analysis

The transcribed material was analyzed using qualitative content analysis. An inductive coding scheme was developed to identify recurring themes. The analysis focused on clustering insights into threat types, attack feasibility, system weaknesses, and organizational practices. These categories informed the structure and content of the subsequent results and discussion sections.

While this study is grounded in qualitative analysis due to the domain's sensitivity and expert-driven nature, future extensions could explore quantitative methodologies such as the Common Vulnerability Scoring System (CVSS), probabilistic threat trees, or hybrid models in aviation. The assessed risks in this paper are based on preliminary efforts in this direction. The simplified versions (cf. Tables II, III, IV, and V) are related to pilot-centered studies using ICAO Doc 9859-compliant matrices [11], offering a valuable foundation for quantitative risk propagation modeling in aviation cybersecurity.

III. Threat Landscape

Understanding the diverse threat landscape is critical for developing effective cybersecurity strategies in civil aviation. Cybersecurity threats in aviation are evolving with the increasing digitization and integration of ICT tools [10], smart technologies and IoT devices in airports [4]. The aviation sector is confronted by a range of adversaries, each with different motives, capabilities, and targets. This section provides an overview of the primary threat actors and analyzes their motivations and technical capacities.

A. Overview of Threat Actors

Nation-state actors are considered among the most capable and persistent adversaries, pose significant risks to aviation systems, targeting communication networks and avionics for political influence and intelligence gathering [8], [12], [13]. Their motivations typically include political influence, economic disruption, and strategic intelligence gathering. These actors, often operating as Advanced Persistent Threat (APT) groups, have access to substantial resources and engage in long-term operations [10]. The complexity and interconnectedness of Communication, Navigation, and Surveillance (CNS) infrastructure amplify the potential scope of attacks [14]. This includes communication networks, air traffic control infrastructure, or avionics systems [10], [15].

Cybercriminals and hacktivists often exploit known vulnerabilities for financial gain or ideological purposes [4], [16]. Airports and airlines face various cyber risks, including potential loss of passenger information, disruption of operations, and damage to aircraft [17]. Ransomware attacks on airport IT systems and attempts to breach airline customer databases are common examples. Hacktivists may seek to disrupt flight operations or expose perceived injustices using defacement, denial-of-service (DoS) attacks, or information leaks [10], [18].

Insider threats pose a significant cybersecurity risk, often underestimated compared to external attacks [19]. These threats come from individuals with legitimate access, such as employees, contractors, or vendors, who may exploit their knowledge of internal systems and bypass perimeter defenses. The impact of insider attacks can be severe, as evidenced by high-profile cases at companies like Tesla and government agencies like the US Department of Defense [20]. Insiders are particularly dangerous due to their operational knowledge and ability to bypass conventional perimeter defenses [21].

B. Motivations and Capabilities

Threat actors targeting civil aviation operate with a broad spectrum of motivations:

- **Political motivations:** Aimed at destabilizing nations, projecting power, or coercing policy changes (nation-states) [22], [23].
- **Economic motivations:** Including theft of personal data, ransom payments, or illicit trade in sensitive information (cybercriminals) [4], [10].
- **Ideological motivations:** Related to activist agendas or grievances against the aviation industry (hacktivists) [15], [16].

Their capabilities vary widely. Nation-states can exploit zero-day vulnerabilities and conduct coordinated cyber-physical operations [24]. Cybercriminals often rely on off-the-shelf malware and social engineering, whereas insiders leverage their access privileges and domain familiarity to perform covert actions [21]. All actors are increasingly capable of targeting key aviation subsystems, including avionics, ground control centers, and satellite communication links [25].

Table I presents a summary of selected real-world aviation cybersecurity incidents that illustrate the feasibility and impact of documented vulnerabilities.

TABLE I
SELECTED CYBERSECURITY INCIDENTS IN CIVIL AVIATION

Year	Incident	Vector	Impact
2018	Brit. Airways breach	Customer DB	Data theft (£20M)
2020	Ransomware on ST Eng.	Airport MRO	Operations halt
2023	GNSS spoofing Iraq/Iran	GNSS	Position deviat.
2024	Hamburg airport cam. hack	IT system	Public data leak

IV. ATTACK VECTORS AND VULNERABILITIES

This section synthesizes the findings from expert interviews with a literature-based analysis, providing a structured overview of the main attack vectors in civil aviation. It follows the categories of airborne systems, ground infrastructure, and communication links. The complex interplay between airborne, ground, and communication subsystems is illustrated in Figure 1, which highlights how interdependencies across aviation infrastructure expand the cyber attack surface.

The tables (cf. Table II, III and IV) reflect the prioritization of threats as described by expert interviewees and supported by the literature review. In detail, the attack vectors discussed below are derived from a thematic synthesis of the expert interviews and the structured literature review. Key vulnerabilities were categorized where at least two interviewees identified similar risks, which were then cross-validated against peer-reviewed and industry literature. This integration follows principles of inductive qualitative coding and thematic saturation, ensuring methodological rigor in capturing domain knowledge. The likelihood and impact ratings are derived through a triangulated synthesis of literature and practitioner input. Attack vector tables are annotated with expert-based (E), literature-based (L), or combined evidence (E+L), to clarify the provenance of each rating.

A. Airborne Systems

Airborne systems include all onboard digital subsystems, such as avionics, navigation, and communication modules.

Figure 1. Interlinked Systems in Civil Aviation [26]

TABLE II
RISKS IN AIRBORNE SYSTEMS

Attack Vector	Likelihood	Impact	Evidence
Legacy avionics exploitation	Medium	High	E+L
SATCOM command injection	Medium	High	E+L
ADS-B ghost aircraft injection	High	High	E+L
GNSS spoofing/jamming	High	High	E+L

Experts emphasized the high dependency of modern aircraft on complex, interconnected technologies, many of which were not originally designed with cybersecurity in mind. The summary of the risks for airborne systems is shown in Table II.

1) Avionics and Flight Management Systems: Legacy avionics platforms often operate on proprietary or outdated software with limited patching capabilities due to certification constraints [27]. These systems are vulnerable to local and remote exploitation if attackers gain access to maintenance ports or use wireless vectors during pre-flight servicing [28], [29]. According to expert interviews and industry reports, exploitation is considered *moderately likely*, but the *impact is high* due to the proximity of these systems to flight-critical functions.

2) SATCOM and Data Links: SATCOM-based communication plays a central role in long-haul aviation [30]. Experts highlighted that many implementations lack strong encryption or robust authentication, exposing them to spoofing or hijacking attempts [31]. Attackers could theoretically disrupt the data integrity between cockpit and ground services or inject false control commands [30]–[32]. Although complex, such attacks are *technically feasible*, making the *likelihood medium* and the *impact high* due to the potential for operational disruption.

3) ADS-B and GNSS: The ADS-B protocol broadcasts aircraft position data in plaintext, without encryption or authentication [31], [32]. This allows attackers to eavesdrop or inject ghost aircraft into air traffic visualizations [31], [33]. GNSS signals are also weak and susceptible to jamming or spoofing, which can mislead navigation systems [34], [35].

TABLE III
RISKS IN GROUND INFRASTRUCTURE

Attack Vector	Likelihood	Impact	Evidence
Ransomware in airport IT	High	Medium	E+L
ATM network compromise	Medium	High	E+L
Third-party lateral movement	High	Medium	E
Manipulated maintenance records	Medium	High	E+L

TABLE IV
RISKS IN COMMUNICATION LINKS

Attack Vector	Likelihood	Impact	Evi.
ACARS interception	High	Medium	E+L
ACARS message manipulat.	Medium	High	E+L
SWIM data injection	Medium	Medium–High	E+L
VHF/UHF spoofing or jam.	Low–Medium	Medium	E+L

Several real-world incidents (Middle East) validate feasibility [15], [36], [37]. These attacks are *well-documented in research and red-teaming efforts*, making the *likelihood high* and the *impact high*.

B. Ground Infrastructure

Ground-based systems provide essential support for aircraft operations, including logistics, passenger processing, and air traffic control. The following subsystems were identified as critical and the summary of the risks for ground infrastructure is shown in Table III.

1) Airport IT Systems and Networks: Experts reported that airport IT systems are often heterogeneous and difficult to centrally manage [4]. Attack vectors include ransomware, spear-phishing, and lateral movement via third-party contractor access [15], [18]. Ransomware attacks have frequently occurred globally (e.g., ransomware at airport check-in systems) [38], [39], confirming the *high likelihood* also due to weak endpoint protection, though the *impact is considered medium* as the attacks typically affect business continuity rather than flight safety.

2) ATM Systems: Air traffic control environments rely on legacy architectures and software as well as centralized infrastructures [40]. Experts warned that insufficient network segmentation and outdated authentication mechanisms pose severe risks, especially when connected to supervisory control and data acquisition systems [41]. Experts cite complex vendor ecosystems [18]. Access is often poorly segmented, and attackers can escalate privileges across IT networks [42]. The *likelihood is medium* due to controlled access, while the *impact is high* because compromised ATM systems could disrupt national airspace by impacting flight routing, a safety-critical function. Operational disruption in ATM may lead to cascading scheduling effects that indirectly compromise flight safety and emergency response coordination.

3) Supply Chain and Maintenance Systems: Digital systems used for aircraft maintenance, such as electronic logbooks and maintenance management tools, were identified as vulnerable due to limited access control and shared interfaces [27], [42]. Digital systems are exposed via remote or wireless interfaces [43]. If exploited, could lead to incorrect repairs or overlooked issues that allow subtle manipulation of aircraft safety-related data [44]. The *likelihood is medium*, and the *impact is high* due to latent threats to airworthiness.

C. Communication Links

Cybersecurity vulnerabilities in communication links were a key concern across all interviews and the summary of the risks for communication links is shown in Table IV.

1) ACARS and Voice Communications: The ACARS transmits sensitive data like flight plans, fuel status and weather updates over plaintext VHF or SATCOM channels [45], [46]. Experts warned of the ease with which such messages can be intercepted or crafted valid messages can be injected into systems using low-cost software-defined radios [31], [33]. This results in a *high likelihood* for data interception, and a *medium impact* as the intercepted data could support more targeted or disruptive attacks.

2) SWIM and IP-based Protocols: The increasing adoption of System Wide Information Management (SWIM) introduces standardized interfaces for data exchange between aviation actors using standardized APIs over IP [40]. However, this integration also extends the attack surface, especially when IP-based protocols are used without end-to-end encryption [15], [47]. Improper authentication may allow false data exchange (e.g., flight status, weather) [31]. While no public exploitation is known to date, *expert opinion assessed the likelihood as medium* and the *impact as medium to high*, depending on the data affected.

D. Summary of Findings

The aggregated results from expert interviews and supporting literature indicate that cyber risks in civil aviation vary significantly across system categories in both likelihood and potential impact, cf. Table V.

Airborne systems — particularly those relying on outdated avionics or unauthenticated data broadcasts such as ADS-B — were consistently rated as having the highest impact, given their direct connection to flight safety and the limited ability to implement rapid updates due to certification constraints. However, due to more restricted physical and logical access, the likelihood of successful exploitation was generally considered medium to high.

Ground infrastructure, encompassing airport IT, ATM networks, and maintenance systems, presented a higher likelihood of exploitation. This was attributed to the widespread use of commercial off-the-shelf (COTS) components, heterogeneous networks, and extensive third-party integration. Although the immediate safety impact of attacks on ground systems may be lower, operational disruptions and indirect safety effects — such as delayed maintenance updates — elevate the risk severity.

Communication links were assessed to have a medium likelihood of exploitation due to known vulnerabilities in protocols like ACARS and the integration of IP-based systems like SWIM. Experts emphasized that while direct safety effects depend on the attack vector, compromised communication

integrity could result in degraded situational awareness or operational delays.

TABLE V
RISK OVERVIEW BY ATTACK VECTOR CATEGORY

Category	Likelihood	Impact	Evi.
Airborne Systems	Medium–High	High	E+L
Ground Infrastructure	Medium–High	Medium–High	E+L
Communication Links	Low–High	Medium–High	E+L

V. DISCUSSION

This study aimed to provide a comprehensive assessment of cybersecurity threats in civil aviation by combining expert insights with a structured vulnerability evaluation. Unlike prior studies, this paper introduces a layered risk prioritization based on operational pilots' judgment integrated with literature-based scoring. The findings confirm that the aviation sector is facing a complex, multi-dimensional threat landscape characterized by both well-understood and emerging attack vectors.

A. Expert Consensus and Divergences

Across the interviews, there was broad consensus regarding the most critical vulnerabilities: unauthenticated communication protocols (especially ADS-B and ACARS), outdated avionics platforms, and ransomware threats in ground infrastructure. Experts agreed that while the likelihood of attacking airborne systems may be lower due to restricted access and specialized knowledge requirements, the potential impact is significantly higher due to safety-critical dependencies. Conversely, ground systems are more exposed due to extensive third-party integration and reliance on legacy IT architectures.

A distinguishing contribution of this study lies in its triangulated risk synthesis, which not only validates known attack vectors such as ADS-B spoofing and ACARS plaintext but also stratifies their risk severity based on direct expert evaluation. Unlike prior literature reviews, this paper systematically ranks vulnerabilities across airborne, ground, and communication layers, reflecting real-world operator prioritization and threat perception.

Notably, the perception of risk around communication systems varied more significantly among experts. Some emphasized the high exploitability of ACARS and voice channels due to lack of encryption, while others viewed such channels as low-priority targets, arguing that operational redundancy limits their criticality. This divergence points to the need for scenario-based risk modeling to clarify the consequences of link-level compromises.

B. Identified Security Gaps

The results presented in Section IV highlight how cyber threats manifest across system layers. Rather than restating attack vectors, we group observed weaknesses into four overarching categories: (1) legacy systems lacking patchability, (2) insecure-by-design communication protocols, (3) unsegmented network architectures, and (4) limited visibility across operational technology (OT)/IT domains. These categories are not isolated — their interdependencies intensify systemic risk. For example, outdated avionics in airborne systems not only lack encryption but also interact with unverified ground data over ADS-B and SATCOM, compounding threat exposure.

- **Legacy technology**: Many components in avionics and air traffic systems remain unpatched or unsupported, yet are essential to certified aircraft and control operations.
- **Protocol weaknesses**: Unsecured communications (e.g., ADS-B, ACARS) are still in widespread use without industry-wide mandates for cryptographic protection.
- **Insufficient segmentation**: Airport and ATM networks often lack adequate isolation between OT and IT systems, allowing lateral movement in case of breach.
- **Limited situational awareness**: There is a notable gap in the deployment of real-time intrusion detection or anomaly recognition systems tailored for aviation environments.

Synthesizing the results reveals that many risks cannot be addressed at the subsystem level alone. Vulnerabilities in airborne platforms (e.g., legacy flight systems) are often mirrored by insecure communications (e.g., unencrypted ACARS) and exacerbated by permissive ground networks (e.g., shared maintenance IT). These layers form a tightly coupled threat surface where mitigation strategies must be holistic rather than component-specific.

C. Organizational and Regulatory Challenges

Beyond technical vulnerabilities, organizational barriers emerged as a dominant theme. Experts noted that aviation cybersecurity is hindered by inter-organizational complexity and unclear accountability across airline operators, airport authorities, OEMs, and regulators. This diffusion of responsibility contributes to delayed patch cycles, inconsistent incident reporting, and fragmented responses to shared threats.

From a regulatory perspective, initiatives such as the ICAO Cybersecurity Strategy and EASA's oversight programs have made progress in establishing a governance framework. However, practical enforcement and harmonized adoption across countries and actors remain lacking. Several interviewees stressed the importance of moving from voluntary guidance to enforceable minimum cybersecurity baselines, particularly for data integrity and access control in ground-air-ground communication.

D. Strategic Implications

Taken together, the results highlight the need for a layered and aviation-specific cybersecurity approach. Mitigation strategies must prioritize:

- Protection of safety-critical systems (e.g., navigation, control) through isolation and redundancy.
- Gradual deprecation of insecure communication protocols in favor of authenticated, encrypted alternatives.
- Continuous training and threat modeling across operational teams, IT personnel, and aircrew.
- Strengthening of information sharing platforms for threat intelligence between stakeholders.

The findings also support the adoption of advanced monitoring tools (e.g., AI-based intrusion detection) to detect anomalous patterns across OT and IT boundaries. While technical interventions are necessary, a cohesive security culture supported by policy and cross-organizational cooperation is essential to sustaining trust in civil aviation infrastructure.

VI. Conclusion and Future Work

A. Conclusion

This paper investigated the cybersecurity threat landscape in civil aviation by answering three guiding research questions. In addressing RQ1, the study identified nation-states, cybercriminals, and insiders as the principal threat actors. Nation-state adversaries were considered the most capable, often motivated by political or strategic objectives, while cybercriminals targeted economic assets through extortion or data theft. Insider threats, although less visible, remain dangerous due to their system knowledge and access privileges.

For RQ2, the study systematically categorized attack vectors across three critical domains: airborne systems, ground infrastructure, and communication links. Particular emphasis was placed on unauthenticated data links such as ADS-B and ACARS, insecure SATCOM implementations, and legacy airport IT systems. These vectors were identified through both expert elicitation and evidence from past incidents, supporting their relevance and severity.

Addressing RQ3, the research showed that civil aviation systems remain highly vulnerable to cyberattacks. Vulnerabilities were not limited to outdated technologies, but also to organizational fragmentation and limited situational awareness across stakeholders. While the impact of an attack on airborne systems is typically higher due to safety implications, ground and communication systems were found to be more accessible, increasing the likelihood of compromise.

B. Recommendations

Based on these results, the following recommendations are proposed. Each is explicitly linked to the corresponding research question (RQ) to ensure coherence and traceability:

RQ1 (Threat Actors): Aviation regulators and industry actors should establish mandatory information-sharing frameworks and joint cyber exercises to enhance situational awareness and resilience across organizational boundaries. These measures address the complex threat actor landscape — ranging from state-sponsored APTs to insider threats — by strengthening collaborative defense mechanisms and reducing organizational silos.

RQ2 (Attack Vectors): The adoption of secure communication protocols, such as encrypted ADS-B, IP-authenticated SWIM, and secure ACARS variants, must become mandatory. These steps directly mitigate attack vectors that exploit unauthenticated or plaintext messaging formats, which are prevalent in both airborne and ground-air communication systems.

RQ3 (System Vulnerability): Addressing systemic vulnerabilities requires both technical retrofitting and architectural modernization. Legacy avionics and airport IT systems must be upgraded using secure-by-design principles despite long certification cycles. In parallel, strict network segmentation and anomaly detection tailored to OT/IT hybrid environments should be deployed to detect and contain threats across domain boundaries. These controls improve visibility into lateral movements and cross-layer attacks, especially in supply chain and maintenance subsystems.

Strategic Roadmap for Mitigation: To operationalize the recommendations and support implementation across the aviation sector, a phased roadmap is proposed. This roadmap spans short-, mid-, and long-term actions, corresponding to technical, infrastructural, and governance domains:

In the short term, priority should be given to securing vulnerable communication protocols. This includes deploying encryption and authentication mechanisms for ADS-B and ACARS transmissions, as well as enforcing strict access control policies for SWIM interfaces.

In the mid term, focus must shift to infrastructure hardening. Key actions involve segmenting ATM and airport IT networks to reduce lateral movement risk, and upgrading airport systems that currently rely on outdated or unsupported software components.

In the long term, sustainable cybersecurity in civil aviation requires robust governance mechanisms. These include mandatory coordinated vulnerability disclosure programs, harmonized reporting obligations across national aviation authorities, and alignment with international cybersecurity baselines as advocated by ICAO and EASA.

C. Future Work

Quantitative modeling and simulation frameworks should be developed to better understand risk propagation and system dependencies across aviation domains. These models can support scenario-based planning and incident response.

Advanced machine learning techniques offer potential for anomaly detection in avionics and ATM environments. Research should explore real-time inference models that account for context, latency, and safety constraints.

Policy-oriented studies are needed to evaluate how regulatory mandates, certification policies, and governance frameworks influence cybersecurity readiness across aviation actors.

Lastly, comparative analyses across critical infrastructure sectors (e.g., rail, maritime, energy) can identify transferable best practices and highlight aviation-specific requirements for cybersecurity resilience.

In summary, this research confirms that civil aviation cybersecurity is a multi-dimensional challenge requiring coordinated technical, organizational, and regulatory responses. Mitigating these threats demands not only improvements in system design and risk detection, but also sustained governance, industry-wide collaboration, and a proactive security culture embedded across all aviation stakeholders.

References

[1] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE transactions on intelligent transportation systems*, vol. 18, no. 6, pp. 1338–1357, 2016.

[2] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in digital aeronautical communications a comprehensive gap analysis," *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100549, 2022.

[3] M. Wolf, M. Minzlaff, and M. Moser, "Information technology security threats to modern e-enabled aircraft: A cautionary note," *Journal of Aerospace Information Systems*, vol. 11, no. 7, pp. 447–457, 2014.

[4] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, 2018.

[5] A. A. Elmarady and K. Rahouma, "Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment," *IEEE access*, vol. 9, pp. 143 997–144 016, 2021.

[6] E. Habler, R. Bitton, and A. Shabtai, "Assessing aircraft security: A comprehensive survey and methodology for evaluation," *ACM Computing Surveys*, vol. 56, no. 4, pp. 1–40, 2023.

[7] A. C. Tang, "A review on cybersecurity vulnerabilities for urban air mobility," in *Aiaa scitech 2021 forum*, 2021, p. 0773.

[8] G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K. R. Choo, "Cyber security challenges in aviation communication, navigation, and surveillance," *Computers & Security*, vol. 112, p. 102516, 2022.

[9] C. A. P. Viveros, "Analysis of the cyber attacks against ads-b perspective of aviation experts," *Master's thesis, University of Tartu*, 2016.

[10] E. Ukwandu, M. A. Ben-Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, I. Andonovic, and X. Bellekens, "Cyber-security challenges in aviation industry: A review of current and future trends," p. 146, 2022.

[11] I. Doc, "ICAO Doc 9859 safety management manual," *Montreal: International Civil Aviation Organization*, 2018.

[12] A. Pawlicka, M. Choraś, and M. Pawlicki, "Cyberspace threats: not only hackers and criminals. raising the awareness of selected unusual cyberspace actors-cybersecurity researchers' perspective," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–11.

[13] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology innovation management review*, vol. 4, no. 10, 2014.

[14] Y. Xie, A. Gardi, and R. Sabatini, "Cybersecurity risks and threats in avionics and autonomous systems," in *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2023, pp. 0814–0819.

[15] A. Malatras, Z. Stanic, I. Lella, R. De Sousa Figueiredo, E. Tsekmezoglou, M. Theocharidou, R. Naydenov, and A. Drougkas, "Enisa threat landscape: Transport sector (january 2021 to october 2022)," 2023.

[16] J. Soldatos, J. Philpot, and G. Giunta, "Cyber-physical threat intelligence for critical infrastructures security: a guide to integrated cyber-physical protection of modern critical infrastructures," 2020.

[17] A. Alsaidi, A. Gutub, and T. Alkhodaidi, "Journal of forensic research," 2019.

[18] B. I. Scott, "Aviation cybersecurity: Regulatory approach in the european union," 2019.

[19] J. Predd, S. L. Pfleeger, J. Hunker, and C. Bulford, "Insiders behaving badly," *IEEE Security & Privacy*, vol. 6, no. 4, pp. 66–70, 2008.

[20] G. Mazzarolo and A. D. Jurcut, "Insider threats in cyber security: The enemy within the gates," *arXiv preprint arXiv:1911.09575*, 2019.

[21] B. Bean, "Mitigating insider threats in the domestic aviation system: Policy options for tsa," 2017.

[22] R. Abeyratne, "Cyber terrorism and aviation—national and international responses," pp. 337–349, 2011.

[23] A. F. Brantly, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 edited by Jason Healy: Arlington, VA: Cyber Conflict Studies Association*. Taylor & Francis, 2014.

[24] M. C. Libicki, *Conquest in cyberspace: national security and information warfare*. Cambridge University Press, 2007.

[25] K. Sampigethaya and R. Poovendran, "Aviation cyber-physical systems: Foundations for future aircraft and air transport," *Proceedings of the IEEE*, vol. 101, no. 8, pp. 1834–1855, 2013.

[26] P. Gontar, H. Homans, M. Rostalski, J. Behrend, F. Dehais, and K. Bengler, "Are pilots prepared for a cyber-attack? a human factors approach to the experimental evaluation of pilots' behavior," *Journal of Air Transport Management*, vol. 69, pp. 26–37, 2018.

[27] R. De Cerchio and C. Riley, "Aircraft systems cyber security," pp. 1C3–1, 2011.

[28] E. Habler, R. Bitton, and A. Shabtai, "Evaluating the security of aircraft systems," *arXiv preprint arXiv:2209.04028*, 2022.

[29] L. Bogoda, J. Mo, and C. Bil, "A systems engineering approach to appraise cybersecurity risks of cns/atm and avionics systems," in *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, 2019, pp. 1–15.

[30] S. Khare and N. S. Talwandi, "Satellite communication vulnerabilities and threat landscape," in *2024 IEEE Silchar Subsection Conference (SILCON 2024)*. IEEE, 2024, pp. 1–6.

[31] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2014.

[32] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings 11*. Springer, 2013, pp. 253–271.

[33] A. Costin, A. Francillon *et al.*, "Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices," pp. 1–12, 2012.

[34] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *University of Texas at Austin (July 18, 2012)*, pp. 1–16, 2012.

[35] M. L. Psiaki and T. E. Humphreys, "Gnss spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[36] D. Sullivan, "Above us only stars: Exposing gps spoofing in russia and syria," https://c4ads.org/publications/above-us-only-stars, 2019, c4ADS Report [retrieved: February, 2025].

[37] GPSJam.org, "Global gps interference map - crowdsourced gnss disruption data," https://gpsjam.org, 2024, [Retrieved: April, 2025].

[38] A. Lawall and P. Beenken, "A threat-led approach to mitigating ransomware attacks: Insights from a comprehensive analysis of the ransomware ecosystem," in *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, ser. EICC '24, S. Li, K. Coopamootoo, and M. Sirivianos, Eds. New York, NY, USA: Association for Computing Machinery, 2024, p. 210–216. [Online]. Available: https://doi.org/10.1145/3655693.3661321

[39] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "A holistic review of cybersecurity and reliability perspectives in smart airports," *IEEE Access*, vol. 8, pp. 209 802–209 834, 2020.

[40] R. Medina, "Air traffic management (atm)," Cairn/Cairn, pp. 22–27, 2024.

[41] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "Guide to industrial control systems (ics) security," National Institute of Standards and Technology, Tech. Rep. 82, 2011.

[42] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, and T. Baker, "Security threats to critical infrastructure: the human factor," *The Journal of Supercomputing*, vol. 74, pp. 4986–5002, 2018.

[43] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on emerging topics in computing*, vol. 5, no. 4, pp. 586–602, 2016.

[44] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[45] X. Lu, "Research on the security of communication addressing and reporting system of civil aircraft," in *IOP Conference Series: Earth and Environmental Science*, vol. 295, no. 3. IOP Publishing, 2019, p. 032026.

[46] A. Roy, "Secure aircraft communications addressing and reporting system (acars)," in *20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219)*, vol. 2. IEEE, 2001, pp. 7A2–1.

[47] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 3–11, 2013.